**Cyber Security Advisories**

**Date: 30 November 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-P-112024264 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-290112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P112024074 A critical unauthenticated RCE vulnerability in the Palo Alto PAN-OS management interface |  |  |  |
|  | CMTX-I-993112024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-295112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-112024794 Cumulative Suspicious Domains--ALERT2 |  |  |  |
|  | CMTX-P-112024274 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024284 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-401112024 ActionRAT Malware- Threat Actor: SideCopy |  |  |  |
|  | CMTX-P-112024074 PXA Stealer |  |  |  |
|  | CMTX-I-281112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-053112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-257112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P112024994 Relay server Nodes used by Chinese actors--ALERT11 |  |  |  |
|  | CMTX-P-112024038 Critical Alert: Helldown Ransomware |  |  |  |
|  | CMTX-P-112024048 Earth Kasha Threat Actor Campaign |  |  |  |
|  | CMTX-P-112024814 Cumulative Suspicious Domains--ALERT3 |  |  |  |
|  | CMTX-I-388112024 Malicious Domain Typo-Squatting CBI Domain used by Threat Actors |  |  |  |
|  | CMTX-P-112024324 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-981112024 Malicious Sub-Domains- Possibly Phishing |  |  |  |
|  | CMTX-P-112024904 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024804 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-355112024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P112024605 ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2023-28461) AFFECTING ARRAY NETWORK |  |  |  |
|  | CMTX-P112024705 Chinese APT "Earth Estries" Targeting Critical Infrastructure with New Attack Vectors and New Backdoor Malwares |  |  |  |
|  | CMTX-P-TL-1120243214 Notable Tunneling Tools leveraged by state sponsored/ ransomware actors |  |  |  |
|  | CMTX-I-770112024 AsyncRAT Malware |  |  |  |
|  | CMTX-I-070112024 Malicious Domain- Spear-Phishing |  |  |  |
|  | CMTX-P-112024394 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024404 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-112024824 Cumulative Suspicious Domains--ALERT4 |  |  |  |